REMARKS

This Amendment is filed in response to the Office Action mailed Jan. 9, 2009 in connection with a Petition for a 1-month Extension of Time. The Applicant respectfully requests reconsideration. All objections and rejections are respectfully traversed.

Claims 1-32 are pending in the application.

No claims have been added or amended,

Claim Rejections - 35 U.S.C. §102

At paragraphs 11-21 of the Office Action, claims 1-4, 8, 14, 18, 21, 24 and 29-32 were rejected under 35 U.S.C. §102(a) and §102(e) over Richmond et al., U.S. Publication No. 2003/0152067 (hereinafter "Richmond").

Claims 1-2, 4, 8, 14, 18, 21, 24, 29, 30 and 32:

The Applicant's claim 1, representative in part also of claims 2, 4, 8, 14, 18, 21, 24, 29, 30 and 32, sets forth (emphasis added):

> 1. A method for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being a physical interface coupled to a plurality of client nodes, the method comprising:
>
> ***partitioning the shared media port into a plurality of logical subinterfaces***, wherein a logical subinterface is a logical division of a physical interface, ***each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node***;
>
> receiving a data packet at the shared media port from a first client node;
>
> associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces;
>
> ***determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork***;
>
> if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnet-

work, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork;

receiving a second data packet at the shared media port from a second client node;

associating the second received data packet with the first logical subinterface;

determining whether the second client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork; and

if the second client node is determined to not be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork, preventing the second received data packet from being forwarded over the first logical subinterface's dedicated network or subnetwork, while still allowing data packets from the first client node to be forwarded if the first client node is determined to be authenticated.

Richmond discusses an network entry device 116 where "[m]ultiple user devices may concurrently exchange packets with [a] port module 118 using communication channels...." *See* paragraph 0023, lines 4-6 and Fig. 1A. The port module 118 may host "a plurality of virtual ports, each virtual port corresponding to one of the communications channels" leading to a user and user device. *See* paragraphs 0023, lines 9-11, paragraphs 0008 and 0264 and Fig. 1A. "Thus each virtual port may be dedicated to a particular user and user device...." *See* paragraph 0264, lines 18-19.

Richmond further discusses that an "[a]uthentication module 1506 may be configured to perform authentication in accordance with one or more authentication technologies, for example RADIUS, a NOS, and IEEE 802.1X." *See* paragraph 0274, lines 1-4. Packets received at the port module 118 of the network entry device 116 may be subject to the authentication.

First, the Applicant respectfully urges that Richmond does not suggest the Applicant's claimed "***partitioning the shared media port into a plurality of logical subinterfaces... each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node***."

While the Applicant partitions a shared media port into logical subinterfaces that **are each dedicated to providing access to a different network or subnetwork accessible through the intermediate node**, Richmond simply establishes **virtual ports dedicated to particular users and user devices**. *See* Richmond paragraph 0264. That is, Richmond's virtual ports are not dedicated to network or subnetwork **accessible through** Richmond's network entry device 116. Rather, Richmond's virtual ports are dedicated to different users and user devices that may be coupled Richmond's network entry device 116, and are attempting to get access to networks or subnetworks behind it. Since Richmond's virtual ports are dedicated to a quite different thing than the Applicant's logical subinterfaces, they may not fairly be equated to the claimed logical subinterfaces.

Such distinction may be better understood by reference to illustrative examples. The Applicant respectfully directs the Examiner's attention to Applicant's Fig. 3, which illustrates an example shared media port 300 of an intermediate node 200, partitioned into two example logical subinterfaces 340, 350. Each example logical subinterface is dedicated to providing access to a different network or subnetwork accessible through the intermediate node. For instance, example logical subinterface 340 is dedicated to providing access to Enterprise VPN 155 that is accessible through the intermediate node. Similarly, example logical subinterface 350 is dedicated to providing access to the Internet. Thus, depending on which network or subnetwork a user desires to access, the user will attempt to access a different logical subinterface.

The Applicant further respectfully directs the Examiner's attention to Fig. 1A of Richmond, which illustrates a contrasting type of operation. As shown in Fig. 1A, port module 118 of network entry device 116 includes virtual ports that each correspond to a communication channel leading to a different user and user device. "Thus each virtual port may be dedicated to a particular user and user device...." *See* paragraph 0264, lines 18-19. Richmond's virtual ports are not dedicated to different networks accessible through/behind Richmond's network entry device 116. Further, user devices in Richmond do not attempt to access different virtual ports depending on which networks or subnetworks they want to access.

Accordingly, for the reasons discussed above, the Applicant respectfully urges that Richmond does not anticipate the claimed "***partitioning the shared media port into a plurality of logical subinterfaces... each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node***" under 35 U.S.C. §102.

Second, the Applicant respectfully urges that Richmond does not suggest the Applicant's claimed "***determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork***."

Since Richmond does not disclose structures akin to the claimed logical subinterfaces (i.e., Richmond's virtual ports are not akin to logical subinterfaces), Richmond may not fairly be interpreted as teaching determining whether a client node is authenticated to communicate over a logical subinterface's dedicated network or subnetwork. Richmond merely mentions that an authentication module may be configured to perform authentication on packets received at a port module. Richmond makes no mention of authentication being performed at the logical subinterface level.

Accordingly, the Applicant respectfully urges that Richmond does not anticipate the claimed "***determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork***" under 35 U.S.C. §102.

Claims 3 and 31:

The Applicant's claim 3, representative in part also of claim 31, sets forth (emphasis added):

> 3. The method according to claim 1, wherein ***the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN)***.

While Richmond mentions that a VPN may be established across networks (*see* Richmond paragraph 0036), Richmond does not suggest that one of his virtual ports

should be dedicated to a providing access to a particular VPN. Instead, as explained above, Richmond's virtual ports are each dedicated to a particular user and user device. *See* Richmond paragraph 0264, lines 18-19. The Applicant respectfully urges that the mere existence of VPN's in Richmond does not suggest a first logical interface being dedicated to providing access to a VPN.

Accordingly, the Applicant respectfully urges that Richmond does not anticipate the claimed "***the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN)***" under 35 U.S.C. §102.

Claim Rejections - 35 U.S.C. §103

At paragraphs 12-25 of the Office Action, claims 5, 9, 11, 15, 17, 19, 22, 23 and 25-28 were rejected under 35 U.S.C. §103(a) over Richmond in view of Kwan et al., U.S. Publication No. 2005/0055570 (hereinafter "Kwan")

The Applicant notes that claims 5, 9, 11, 15, 17, 19, 22 and 23 are dependent claims that depend from independent claims believed to be allowable for at least the reasons discussed above. Claims 5, 9, 11, 15, 17, 19, 22 and 23 are believed to be allowable due to their dependency, as well as for other separate reasons.

Further, the Applicant respectfully urges that claims 25-28 are allowable, at least for reasons similar to those discussed above. The Applicant's claim 25, representative in part also of claims 26-28, sets forth (emphasis added):

> 25. An apparatus comprising:
>
> a shared media port that is a physical interface and has ***a trusted subinterface configured to provide access to a trusted network or subnetwork and an untrusted subinterface configured to provide access to an untrusted network or subnetwork***, wherein a subinterface is a logical division of a physical interface;
>
> an authenticator configured to receive authentication requests from a plurality of client nodes and in response the authentication requests to independently assign to each of the plurality of client nodes an authentication state; and
>
> a media access control (MAC) filter configured to maintain an entry for each client node indicating the authentication state of the client

> node and a MAC address of the client node, and in response to receipt of a data packet from a particular client node directed to the trusted subinterface, to index to an entry in the MAC filter based on a source MAC address of the data packet, to identify the authentication state of the particular client node stored in the indexed MAC-filter entry, and **to *determine whether the particular client node is authenticated to communicate over the trusted subinterface, and, if so, to permit the particular client node to access the trusted subinterface***,
>
> wherein the media access control (MAC) filter grants client nodes access on a client-by-client basis.

The Applicant respectfully urges that neither Richmond nor Kwan suggest the Applicant's claimed "***a trusted subinterface configured to provide access to a trusted network or subnetwork and an untrusted subinterface configured to provide access to an untrusted network or subnetwork***" and "***to determine whether the particular client node is authenticated to communicate over the trusted subinterface, and, if so, to permit the particular client node to access the trusted subinterface.***"

As discussed above, Richmond's virtual ports are not akin to subinterfaces, being associated with users and user devices accessing rather than with networks or subnetworks accessible through an intermediate device. Accordingly, Richmond may not fairly be interpreted as suggesting a trusted subinterface configured to provide access to a trusted network or subnetwork, an untrusted subinterface configured to provide access to an untrusted network or subnetwork, and then performing authentication at the subinterface level.

Such deficiencies in Richmond are not remedied by combination with Kwan. Indeed, the Office Action does not cite to Kwan in relation to these limitations.

Accordingly, the Applicant respectfully requests reconsideration of the rejection of claims 25-28 under 35 U.S.C §103(a) over the combination of Richmond and Kwan.

At paragraphs 26-33 of the Office Action, claims 6 and 10 were rejected under 35 U.S.C. §103(a) over Richmond in view of Kwan, in further view of Ng et al., U.S. Publication No. 2005/0177865 (hereinafter "Ng").

At paragraphs 34-38 of the Office Action, claims 7, 16 and 20 were rejected under 35 U.S.C. §103(a) over Richmond in view of Kwan, in further view of Haverinen et al., U.S. Publication No. 2004/0208151 (hereinafter "Haverinen").

At paragraphs 39-42 of the Office Action, claim 12 was rejected under 35 U.S.C. §103(a) over Richmond in view of Kwan, in further view of Inoue et al., U.S. Patent No. 6,891,819 (hereinafter "Inoue").

At paragraphs 43-46 of the Office Action, claim 13 was rejected under 35 U.S.C. §103(a) over Richmond in view of Kwan, in further view of Roese, U.S. Publication No. 2004/0158735 (hereinafter "Roese").

The Applicant notes that claims 6, 7, 10, 12, 13, 16 and 20 are dependent claims that depend from independent claims believed to be allowable for at least the reasons discussed above. Claims 6, 7, 10, 12, 13, 16 and 20 are believed to be allowable due to their dependency, as well as for other separate reasons.

Should the Examiner believe telephonic contact would be helpful in the disposition of this Application, the Examiner is encouraged to call the undersigned attorney at (617) 951-2500.

In summary, all the independent claims are believed to be in condition for allowance and therefore all dependent claims that depend there from are believed to be in condition for allowance. The Applicant respectfully solicits favorable action.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

/James A. Blanchette/

James A. Blanchette
Reg. No. 51,477
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500